IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/699,005
Filing Date:	10/30/2003
Applicant(s):	Michael Scheidell
Entitled:	INTRUSION DETECTION SYSTEM
Examiner:	Sherkat, Arezoo
Group Art Unit:	2131
Attorney Docket No.:	1012-003U

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellant's Appeal Brief in support of the Notice of Appeal filed March 21, 2008. This Appeal Brief has been timely filed within the statutory period of five months from the filing of the Notice of Appeal, a three month extension of time fee for a petition for a three-month of extension of time is provided herewith. Notwithstanding, please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-3829, and please credit any excess fees to such deposit account.

Date: August 21, 2008

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg, Registration No. 44,725
Customer Number 29973
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Facsimile: (561) 244-1062

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/699,005
Filing Date:	10/30/2003
Applicant(s):	Michael Scheidell
Entitled:	INTRUSION DETECTION SYSTEM
Examiner:	Sherkat, Arezoo
Group Art Unit:	2131
Attorney Docket No.:	1012-003U

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed March 21, 2008, wherein Appellants appeal from the Examiner's rejection of claims 9 through 11 and 14.

I. REAL PARTY IN INTEREST

This application is assigned to SecNAP Network Security, LLC by assignment recorded on October 31, 2002, at Reel 013451, Frame 0050.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1 through 8, 12, 13 and 15 through 20 have been canceled. Claims 9 through 11 and 14 remain pending in this Application and have been three times rejected. It is from the multiple rejections of claims 9 through 11 and 14 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

Claims 9 through 11 and 14 have not been amended since the imposition of the Non-Final Office Action dated November 21, 2007.

V. SUMMARY OF CLAIMED SUBJECT MATTER

As set forth in the Abstract of Appellant's published specification, claims 9 and 14 are directed to an intrusion detection system (IDS). In Appellant's invention, the IDS monitors the rate and characteristics of Internet attacks on a computer network and filters attack alerts based upon various rates and frequencies of the attacks. The IDS also monitors attacks on other hosts and determines if the attacks are random or general attacks or attacks directed towards a specific computer network and generates a corresponding signal. Finally, the IDS tests a computer network's vulnerability to attacks detected on the other monitored hosts.

With specific reference to claim 9, a computer network intrusion detection system can include different log analyzers for different external networks. (Par. [0042]) Each log analyzer can be configured for detecting attacks upon a firewall in a corresponding one of the different external networks defining an edge detection network. (Par. [0042]) An edge database log can be coupled to the different log analyzers logging attacks upon the different external networks.

(Par. [0042]) Further, an intrusion detector can be coupled to a client network and configured to detect external attacks upon the client network. (Par. [0042]) An analyzer also can be coupled to the intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log. (Par. [0045]) Finally, a filter can be coupled to the analyzer for generating an alert based upon characteristics of a plurality of attacks. (Par. [0046])

The system also can include a second intrusion detector for detecting external attacks upon a second computer network. (Par. [0045]) Correspondingly, a second analyzer can be coupled to the second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof. (Par. [0045]) As such, the filter can be further coupled to the second analyzer. (Par. [0045]) When coupled to the second analyzer, the filter further compares the attack characteristics determined by the analyzer and the second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison. (Par. [0045])

With respect to claim 14, a method of generating a network intrusion alert for a first network coupled to a multiple client network system can be provided. (Par. [0047]) The method can include logging attacks on multiple different external networks defining an edge detection network (Par. [0055]), detecting an attack on a client network (Par. [0055]), classifying the attack as either a general attack or a client specific attack (Par. [0055]) by comparing the attack to attacks logged for the edge detection network (Par. [0055]), prioritizing handling of the

detected attack if the attack is classified as a general attack (Par. [0055]), and generating a second alert in response to the presence of the match wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network. (Par. [0055]).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 9 through 11 and 14 are not anticipated by U.S. Patent Application Publiation No. 2002/0178383 by Hrabik et al. (Hrabik) under 35 U.S.C. § 102(e).

VII. THE ARGUMENT

THE REJECTION OF CLAIMS 9 THROUGH 11 AND 14 UNDER 35 U.S.C. § 102(E)

The factual determination of anticipation under 35 U.S.C. § 102 requires the identical disclosure, either explicitly or inherently, of each element of a claimed invention in a single reference.[1] Moreover, the anticipating prior art reference must describe the recited invention with sufficient clarity and detail to establish that the claimed limitations existed in the prior art and that such existence would be recognized by one having ordinary skill in the art.[2] Absence from an allegedly anticipating prior art reference of any claimed element negates anticipation.[3]

"Both anticipation under § 102 and obviousness under § 103 are two-step inquiries. The first step in both analyses is a proper construction of the claims. ... The second step in the

[1] In re Schreiber, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either explicitly or inherently"), In re Rijckaert, 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993); Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); Perkin-Elmer Corp. v. Computervision Corp., 732 F.2d 888, 894, 221 USPQ 669, 673 (Fed. Cir. 1984).

[2] See In re Spada, 911 F.2d 705, 708, 15 USPQ 1655, 1657 (Fed. Cir. 1990); Diversitech Corp. v. Century Steps Inc., 850 F.2d 675, 678, 7 USPQ2d 1315, 1317 (Fed. Cir. 1988).

[3] Kloster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 1571 (Fed. Cir. 1986)(emphasis added).

analyses requires a comparison of the properly construed claim to the prior art."[4] During patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification,"[5] and the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach.[6] Therefore, the Examiner must (i) identify the individual elements of the claims and properly construe these individual elements,[7] , and (ii) identify corresponding elements disclosed in the allegedly anticipating reference and compare these allegedly corresponding elements to the individual elements of the claims.[8] This burden has not been met.

1. Examiner Did Not Comply with the Specificity Requirement of 37 C.F.R. § 1.104(c)(2)

In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.

The importance of the specificity requirement of 37 C.F.R. § 1.104(c) is evident in M.P.E.P. § 706.07, which states:

---

[4] Medichem, S.A. v. Rolabo, S.L., 353 F.3d 928, 933 (Fed. Cir. 2003) (internal citations omitted).

[5] In re ICON Health and Fitness, Inc., 496 F.3d 1374, 1379 (Fed. Cir. 2007) ("[T]he PTO must give claims their broadest reasonable construction consistent with the specification. Therefore, we look to the specification to see if it provides a definition for claim terms, but otherwise apply a broad interpretation."); In re Hyatt, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000).

[6] In re Cortright, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999)

[7] See also, Panduit Corp. v. Dennison Mfg. Co., 810 F.2d 1561, 1567-68 (Fed. Cir. 1987) (In making a patentability determination, analysis must begin with the question, "what is the invention claimed?" since "[c]laim interpretation,. . . will normally control the remainder of the decisional process"); see Gechter v. Davidson, 116 F.3d 1454, 1460 (Fed. Cir. 1997) (requiring explicit claim construction as to any terms in dispute).

[8] Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick Co., 730 F.2d 1452, 221 USPQ 481 (Fed. Cir. 1984).

> The examiner should never lose sight of the fact that in every case the applicant is entitled to a full and fair hearing, and that a clear issue between applicant and examiner should be developed, if possible, before appeal.

A clear issue, however, cannot be developed between Appellant and the Examiner where the basis for the Examiner's rejection of the claims is ambiguous. In the instant case, the Examiner's "analysis" provides little insight as to (i) how the Examiner is interpreting the elements of the claims and (ii) what specific features within Hrabik the Examiner believes identically discloses the specific elements (and interactions between elements) recited in claims 9 through 11 and 14. Rather, on page 2 of the Non-Final Office Action dated November 21, 2007 (the "Non-Final Office Action"),

Examiner provided absolutely no recitation to any portion of Hrabik in connection with the limitation "a plurality of different log analyzers". Further, Examiner referred to a swath of ten (10) paragraphs without specificity in Hrabik in connection with the limitation of "edge database" and "intrusion detector" and another swatch of three (3) paragraphs in connection with the limitation "analyzer" In all instances, **Examiner provided exactly five (5) words of rationale for all of the foregoing!** To that end, Examiner embarrasses the examining corps of the United States Patent and Trademark Office by failing to comply with the most basic responsibilities of the Examiner in performing a proper examination of Appellant's claims.

By failing to specifically identify those features within Hrabik being relied upon in the rejection, the Examiner has essentially forced Appellants to engage in mind reading and/or guessing to determine how the Examiner is interpreting the elements of the claims and what specific features within Hrabik the Examiner believes identically disclose the claimed invention.

2. Examiner Failed to Properly Construe Claim Limitations Integral to the Claims

A critical aspect of Examiner's function as the trier of fact in examining the claims of a patent application is to first perform a claim construction of the terms of the claims. Examiner has failed to expressly do so in the Non-Final Office Action dated November 21, 2007.

A. Claim Construction of Different External Networks

Examiner's comparison of the "target network 100", however, to the claimed limitation of "different external networks" provides an implicit claim construction of "different external networks == a single network"--an obvious error in that the target network is monitored by one or more "security subsystems. A proper claim construction of "different external networks" should be "multiple different external networks".

B. Log Analyzer Detecting Attacks Upon a Firewall

Examiner's comparison of the "security subsystem 50" to a "log analyzer" being "configured to detect attacks upon a firewall" infers Examiner's claim construction of "attacks" as "testing"--another obvious error.[9] Specifically, paragraphs [0043] and [0044] provided in their entirety,

> [0043] During operation, security subsystem 50 monitors the activities of the devices of the target network 100. **Particularly, the critical security-related functions of IDS 18 and firewall 24 are tested. The particular method employed by security subsystem 50 in testing these devices is not critical**, however, the above mentioned approach employing simulated attacks on the components would be suitable.
>
> [0044] **Upon testing the devices, if the integrity of a device on target network 100 cannot be verified, security subsystem 50 reacts.** For example, if IDS 18 has been identified by the subsystem as not reacting properly to attacks on it originating from the internet, appropriate countermeasures could include generating an alert, cutting off or restricting access to the network at firewall 24, or stopping an application. If instead, the firewall is determined not to be

[9] Ironically, the term "log analyzer" appears throughout Hrabik, for example in Figure 4, however, Examiner chooses to read "log analyzer" as it appears in Hrabik on "intrusion detector" rather than "log analyzer" as set forth in Appellant's claims.

> functioning, appropriate action might include disabling access to any servers 14 holding sensitive date. In one possible configuration of the present invention, security subsystem 50 reports network device status to master system 60 which processes the information, and decides on further action. In an alternate configuration, security subsystem 50 is responsible for implementing countermeasures or actions directly. In both cases, however, the results of every test are passed to through any layers of hierarchy to the master system 60 where they are stored for analysis.

At no time are "attacks" detected upon a firewall by security subsystem 50. Rather, the firewall is "tested" as expressly stated in Hrabik. Thus, Examiner has construed "attack" to mean "tested" though the meaning of the term "attack" is well understood and set forth in paragraphs [0002], [0003] and [0013] of Appellant's published specification as follows:

> [0002] A significant problem in the field of computer networks has been the inability to adequately protect private Internet-connected computer networks from **security attacks**. This problem commonly arises, for example when a company interconnects its internal network (typically a local area network) with the Internet to allow company employees to more easily communicate with outside entities. The benefits of connecting the internal network to the Internet are often significant, including, for example, enabling the company to inexpensively disseminate product information and provide online customer support to potential and existing customers.
>
> [0003] As many companies have discovered, however, connecting the internal network to the Internet can have devastating consequences in the absence of an adequate security mechanism. A break-in by a hacker, for example, will often result in the deletion of important data or software files, the introduction of a virus to the network, and/or the public dissemination of confidential information. Less overt break-ins may involve the secret misappropriation of company trade secrets, or the covert manipulation of company data files. Even an innocent act by a company employee, such as the downloading of a virus-ridden file from a Web site, can have devastating effects.
>
> [0013] Intrusion detection follows a simple premise: every network resource and user develops and displays a pattern of normal usage--one that is specific and possibly unique to that item. Though anomalies in network usage sometimes appear, they should be explainable. Anything that cannot be readily explained should be considered a probable attack and investigated. Intrusion detection systems automate much of this process.

Thus, Examiner has misconstrued "attack" and by extension "log analyzer detecting attacks upon a firewall".

C. Edge Database Log

In construing "edge database log", Examiner implicitly equates "edge database log" to "multiple views" in paragraph [0048] of Hrabik which is the only teaching in the swath of paragraphs [0039] to [0048] of Hrabik that relate to the storage of "event information. In doing

so, Examiner completely omits consideration to the term "edge" as expressly recited in Appellant's claims. Yet, paragraph [0042] of Appellant's specification is quite clear on the importance of "edge networks" as they are known in the art. Specifically, in paragraph [0042] it is stated, "Edge networks are known to those familiar with the art and include the edge network.". A proper claim construction "edge database log" would have been "a database log for an edge network".

D. General Attack/Client Specific Attack

In construing the classification of an attack as a general attack or a client specific attack, Examiner compares the claim limitation of "analyzer" to the "LogAnalyzer 504" step of Figure 4 of Hrabik. Paragraph [0057] provides the entirety of teachings in Hrabik relating to the classification of "events" (and not attacks) analyzed in the LogAnalyzer step. Specifically, paragraph [0057] is reproduced in its entirety for the convenience of the Honorable Board:

> [0057] The event classification process (step 170) is accomplished by a classification engine 506. **Once the log analyzer/event consolidator engine has uncovered the source of the event message, the system proceeds to classify the event by determining the overall meaning of the message and specific details necessary to make an evaluation of the significance of the event.** The classification is preferably performed by an event classification engine 506 implemented on the security subsystem. If the classification engine 506 encounters an **unknown type of event**, it immediately uploads the event to the master system 60 for review. In a typical environment, IDS sensors, firewall logs and web logs create a large number of very similar events, many with a minimal security risk. The classification engine will combine these similar messages from different sources, reducing the level of redundancy within the data. Over time, classification engines create and store trending information regarding the types of events occurring most often. Classification engines can then process this information directly without sending these messages up the hierarchy leaving available resources for processing of other potentially important information. The database of event message-types may be incorporated into both the security subsystem and the master system.

Thus, Examiner has implicitly construed "general attack" and "client specific attack" to mean "known type of event" and "unknown type of event". The plain meaning of "general attack" however is an attack that is general in nature, while the plain meaning of "client specific attack" is an attack that is client-specific in nature. The broadest reasonable interpretation of "general

attack" and "client specific attack" set forth above is fully consistent with Appellant's use of the terms in Appellant's specification as evidenced by paragraph [0032] of Appellant's specification as follows:

> [0032] Given the large number of attacks that may be experienced by a client, it is desirable to determine if the attack is a general attack or a specific attack directed at the particular client.

Thus, Examiner has erred in construing the terms "general attack" and "client-specific attack".

3. Examiner Failed to Properly Compare Teachings of Hrabik with Limitations of Claims

For the convenience of the Honorable Board, claims 10 and 11 stand or fall together with claim 9. With respect to claim 9, a computer network intrusion detection system has been recited. A complete reproduction of claim 9 is reproduced herein in its entirety:

> 9. A computer network intrusion detection system comprising:
>
> a plurality of different log analyzers for different external networks, each log analyzer being configured for detecting attacks upon a firewall in an corresponding one of the different external networks defining an edge detection network;
>
> an edge database log coupled to the different log analyzers logging attacks upon the different external networks;
>
> an intrusion detector coupled to a client network and configured to detect external attacks upon the client network;
>
> an analyzer coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log; and,
>
> a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks;
> a second intrusion detector for detecting external attacks upon a second computer network; and,
>
> a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison.

Integral to the system of claim 9 is the inclusion of multiple different log analyzers for different external networks such that each log analyzer is configured for detecting attacks upon a firewall

in a corresponding one of the different external networks. Further integral to the system of claim 9 is the use of an edge database log in an edge detection network. Yet further integral to the system of claim 9 is an analyzer coupled to the intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log. These limitations cannot be found in Hrabik.

Notwithstanding, Examiner argues to the contrary referring non-specifically to a swath of ten paragraphs of Hrabik and an additional three paragraphs. Given Examiner's misconstruction of essential terms present in these integral limitations, Examiner has failed to locate the identical disclosure, either explicitly or inherently, of each element of Appellant's claimed invention in a single reference as required by law. Rather, Examiner only has located a dissimilar disclosure of a system designed to test the integrity of a single network for its ability to handle attacks. **In fact, Hrabik is so dissimilar to Appellant's claimed invention that Hrabik provides absolutely no teaching directed to the classification of attacks detected in multiple different edge networks as either general in nature or client-specific in nature**. Accordingly, Examiner has failed to present a prima facie case of anticipation in respect to claims 9 through 11.

With respect to claim 14, a method of generating a network intrusion alert for a first network coupled to a multiple client network system has been recited. For the convenience of the Honorable Board, a complete reproduction of claim 14 is reproduced herein in its entirety:

> 14. A method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging **attacks** on **multiple** different external networks defining an edge detection network;

detecting an attack on a client network;

classifying the **attack** as either a **general** attack or a **client specific** attack by comparing the attack to attacks logged for the **edge detection network**;

prioritizing handling of the detected attack if the attack is classified as a general attack; and,

generating a second alert in response to the presence of the match wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network.

As was the case in respect to claim 9, Examiner's generic, improper and non-specific reference to a swath of paragraphs with only a modicum of rationale (five words) fails to provide for the identical disclosure, either explicitly or inherently, of each element of Appellant's claimed invention in a single reference as required by law. Notable claim limitations absent from Hrabik include the logging of attacks on multiple different external networks defining an edge detection network and the classification of an attack as either a general attack or a client-specific attack.

In view of the foregoing, Appellant respectfully submits that the Examiner's rejections under 35 U.S.C. § 102(e) based upon the applied prior art are not viable as Examiner has not met Examiner's obligations under 37 C.F.R. § 104(c)(2), as Examiner has completely misconstrued several important claim limitations present in Appellant's claims, and Examiner has failed to compare the properly construed claims to the prior art. Appellants, therefore, respectfully solicit the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 102(e).

Date: August 20, 2008

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg
Registration No. 44,725
Customer Number 29973
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Facsimile: (561) 244-1062

VIII. CLAIMS APPENDIX

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Previously Amended) A computer network intrusion detection system comprising:

a plurality of different log analyzers for different external networks, each log analyzer being configured for detecting attacks upon a firewall in an corresponding one of the different external networks defining an edge detection network;

an edge database log coupled to the different log analyzers logging attacks upon the different external networks;

an intrusion detector coupled to a client network and configured to detect external attacks upon the client network;

an analyzer coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log; and,

a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks;

a second intrusion detector for detecting external attacks upon a second computer network; and,

a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison.

10. (Original) The system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the networks experiencing the attacks having the absence of similarity of attacks on the other of the networks.

11. (Original) The system according to claim 9 further comprising: a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks.

12. (Cancelled)

13. (Cancelled)

14. (Previously Amended) A method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging attacks on multiple different external networks defining an edge detection network;

detecting an attack on a client network;

classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network;

prioritizing handling of the detected attack if the attack is classified as a general attack; and,

generating a second alert in response to the presence of the match wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.